STATE OF ALABAMA

Information Technology Standard

Standard 640-02S1_Rev A: Remote Access Controls

1. INTRODUCTION:

The increasing mobility of State employees and contractors has made remote access to State network resources vital to conducting State business. This standard refines and expands State IT Policy 620-01: Network Access and other relevant policies and standards to address remote access (i.e., any access to the State network through a non-State controlled network, device, or medium).

2. OBJECTIVE:

Ensure remote access technologies are deployed in a manner that ensures State systems maintain acceptable levels of security and service.

3. SCOPE:

These requirements apply to all users (State employees, contractors, vendors, and business partners) who remotely access any State of Alabama information system resources, other than public web servers or systems specifically designed for public access, and to all personnel responsible for the administration of remote access services.

4. REQUIREMENTS:

The following requirements, based the recommendations of the National Institute of Standards and Technology (NIST) found in Special Publication 800-46: Security for Telecommuting and Broadband Communications, apply to remote access connections to State information system resources.

4.1 MANAGEMENT CONTROLS

Access to State network resources from remote locations (including but not limited to homes, hotel rooms, wireless devices and off-site offices) is not automatically granted to users in conjunction with network or system access. State employees and authorized third parties (consultants, vendors, etc.) may utilize remote access capabilities only with written approval of the appropriate authority. Managers shall document access request-approval procedures.

Remote access to sensitive or confidential data requires approval of the data owner and shall comply with the specific requirements of the data owner or of the data type (e.g., Personally Identifiable Information; see applicable State Standard).

Managers and data owners shall review remote access authorizations at least annually.

Revoke remote access authorization when necessary for reasons including, but not limited to, changes in employment, contract termination, non-compliance with security policies, request by the system/data owner, or negative impact on overall network performance attributable to remote access communications.

4.2 ADMINISTRATIVE CONTROLS

The preferred method of remote access to State network resources is through a centrally managed Virtual Private Network (VPN) connection that provides encryption and secure authentication in accordance with State VPN standards.

Do not divulge details or instructions regarding remote access, including external network access points or dial-up numbers except to those requesters that have been verified as authorized to connect to the State network as an external user.

All hosts, including publicly and privately owned personal computers and other remote access devices, connecting remotely to State networks shall have up-to-date and properly configured anti-virus software and current operating system service pack and patch level. Hosts may be scanned to ensure compliance with State standards. Users may be denied remote access if their host system presents an unacceptable risk to State networks.

Place dial-in users under the same access policy as those connecting via VPN by placing the remote access server either in the DMZ or within a screened subnet where the VPN gateway resides.

Secure remote access shall be strictly controlled. Where possible, control will be enforced via one-time password authentication or public/private keys with strong pass-phrases.

With the exception of web servers or other systems where all regular users are anonymous, users are prohibited from remotely logging into any State system or network anonymously (for example, by using “guest” user IDs).

Terminate remote access accounts in accordance with State network and system access policy and standards.

Enforce a limit of not more than 10 consecutive invalid access attempts by a user during a 15 minute time period. The information system shall automatically lock the account/node when the maximum number of unsuccessful attempts is exceeded. Due to the potential for denial of service, automatic lockouts may be automatically released after 15 minutes.

Apply a session time-out that terminates all sessions and requires re-authentication after no more than 15 minutes of inactivity (30 minutes for CICS). Users shall not circumvent this control by deploying automated software mechanisms, or any other strategies, to prevent session time-outs.

Routers for dedicated ISDN lines configured for access to the State network must meet minimum authentication requirements of CHAP.

Dual-homing is not permitted.

4.3 MONITORING

Monitor remote access systems and points of entry to the trusted network to detect unauthorized access attempts and other security weaknesses.

5. DEFINITIONS:

CHAP: Challenge Handshake Authentication Protocol; an authentication method that uses a one-way hashing function.

DUAL HOMING: Network topology in which a device is connected to the network by way of two independent access points (e.g., wired and wireless).

ISDN: Integrated Services Digital Network, a circuit-switched telephone network system that allows digital transmission of voice and data over ordinary telephone copper wires.

6. ADDITIONAL INFORMATION:

6.1 POLICY

Information Technology Policy 640-02: Remote Access

6.2 RELATED DOCUMENTS

Information Technology Policy 620-01: Network and Systems Access

Information Technology Standard 620-01S1: Access Management

Information Technology Standard 640-02S2: Virtual Private Networks

Information Technology Standard 680-01S2: Personally Identifiable Information

Signed by Art Bess, Assistant Director

7. DOCUMENT HISTORY:

Version	Release Date	Comments
Original	2/16/2007	
Rev A	2/20/2008	Changed session time-out from 30 to 15 minutes; changed access authorizations review from quarterly to annually; revised lock-out and monitoring requirements.